UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

Ann Marie Strohm, on behalf of herself and all others similarly situated, **Plaintiff,** **v.** **THE KROGER COMPANY,** **Defendant.**	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Ann Marie Strohm ("Plaintiff"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant The Kroger Company ("Kroger" or "Defendant"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard Kroger's employees' sensitive human resources records, as well as Kroger's customers' personally identifiable information ("PII"), including current and former customer's full names, residential addresses, dates of birth, phone numbers, social security numbers, and its customers' protected health information ("PHI"), including insurance information, prescription information, prescribing doctor, medication names and dates, medical history, medical diagnoses, medical treatment information, and/or clinical history.

2. Kroger is one of the largest supermarket retailers in the United States, headquartered in Cincinnati, Ohio with over 400,000 current employees and over 2,700 locations. It also operates several subsidiary chains including Bakers, City Market, Dillons, Food Co., Food 4 Less, Fred Meyer, Fred Meyers Jewelers, Fry's, Gerbes, Harris Teeter, Home Chef, JayC, King Soopers, The Little Clinic, Mariano's, Metro Market, Owen's, Pay Less, Pick 'n Save, QFC, Ralphs, Roundy's, Ruler Foods, Smith's, and Vitacost. Kroger operates over 2,200 pharmacy locations and an additional roughly 225 Little Clinic locations in the United States making Kroger one of the largest pharmacies in the United States. Furthermore, Kroger provides personal finance and money services to customers and employees throughout the United States.

3. According to Kroger, it was informed on January 23, 2021, that certain of its customers' and employees PII and PHI was disclosed through a data breach involving Kroger's third-party vendor, Accellion. Kroger entrusted its employees' and customers' PII to Accellion for the purposes of transferring certain of Kroger's files and data, including the PII at issue in this matter.

4. Kroger was aware and had full knowledge that Accellion's data security on the platform Kroger used was lax. In fact, prior to the breach, Accellion encouraged Kroger to move to a newer and more secure transfer platform.

5. On February 19, 2021, Kroger mailed data breach notices to those customers and Kroger employees whose PII was accessed by unauthorized third parties. Kroger's February 19, 2021 letter claimed that "No grocery store data was impacted."

6. On March 11, 2021, Kroger mailed a second data breach notice to customers and Kroger employees whose PII was accessed by unauthorized third parties. The March 11, 2021 letter appears to have been sent to a larger group of people than the originally February 19, 2021

letter. Furthermore, the March 11, 2021 letter noticeably did not include the statement that "No grocery store data was impacted."

7. Kroger did not adequately safeguard Plaintiff's data, and now she and apparently many other patients, current and former employees, and customers are the victims of a significant data breach that will negatively affect them for the rest of their lives.

8. Kroger is responsible for allowing this data breach through its failure to implement and maintain reasonable safeguards and its failure to comply with industry-standard data security practices.

9. Despite its role in managing so much sensitive and personal information, Kroger failed to utilize a competent third-party data transfer company when handling and/or transferring Kroger's customers' and current or former employees' PII, and Kroger chose to use an outdated and unsecure transfer platform.

10. Kroger had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access.

11. Plaintiff and those similarly situated rely upon Kroger to maintain the security and privacy of the PII and PHI entrusted to it; when providing their PII and/or PHI, they reasonably expected and understood that Kroger would comply with its obligations to keep the information secure and safe from unauthorized access.

12. In this day and age of regular and consistent data security attacks and data breaches, in particular in the healthcare industry and retail services, Kroger's data security breach is particularly egregious.

13. As a result of Kroger's failures, Plaintiff and the Class Members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

14. Just as their PII and/or PHI was stolen because of its inherent value in the black market, now the inherent value of Plaintiff's and the Class Members' PII and PHI in the legitimate market is significantly and materially decreased.

15. On information and belief, as a result of this massive data breach, at least hundreds of thousands of Kroger's customers and/or current and former employees nationwide have suffered exposure of PII and PHI entrusted to Kroger.

16. In addition, based on Defendant's actions, Plaintiff and the proposed Class have received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Kroger promised when Plaintiff and the proposed Class entrusted Kroger with their PII and PHI.

17. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The injuries suffered by Plaintiff and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the data breach and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to Kroger and with the mutual understanding that Kroger would safeguard Plaintiff's and Class

Members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to Kroger; and (g) the continued risk to their personal data, which remains in the possession of Kroger and which is subject to further breaches so long as Kroger fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' personal data in its possession.

18. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the data breach.

19. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims for breach of implied contract, negligence, negligent entrustment, bailment, and unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Ann Marie Strohm

20. Plaintiff Ann Marie Strohm is a natural person and a resident of Kuna, Idaho. She works at a Fred Meyer store, which is owned by Kroger. In February 2021, Plaintiff received a letter from Kroger dated February 19, 2021 notifying her that her PII had been accessed during Kroger's data breach. In March 2021, she received a second letter from Kroger dated March 11, 2021 notifying her that her PII had been accessed during Kroger's data breach.

21. Plaintiff entrusted her PII and other confidential information such as contact information, financial information and/or Social Security number to Kroger with the reasonable expectation and understanding that Kroger would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or

disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used Kroger's services had she known that Kroger would not take reasonable steps to safeguard her sensitive PII.

22. The letters Plaintiff received dated February 19, 2021 and March 11, 2021, informed her that the PII compromised in the breach included full names, email addresses, and other "contact information" presumably including phone numbers, home address, dates of birth, and also could include salary information.

23. The letters offered to provide her with a limited two-year subscription to the credit monitoring service, Experian. However, this purported remedy is insufficient because it does not prevent or compensate for fraud, but rather monitors for it. Furthermore, the two-year subscription is insufficient as the data included in the breach is permanently compromised. Thus, following the expiration of the two-year subscription, Plaintiff will be forced to pay out of pocket for credit monitoring, which will be necessary the rest of her life.

24. Since learning about the breach, Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of her sensitive personal, financial, and health information.

25. In March 2021, Plaintiff received a letter dated March 5, 2021 from the Idaho Department of Labor notifying her that she had "recently filed for unemployment insurance benefits." But, Plaintiff did not file for unemployment insurance benefits meaning that someone else submitted a claim on her behalf without her authorization.

Defendant Kroger

26. Kroger is a corporation incorporated under the laws of Ohio with its principal place of business in Cincinnati, Ohio.

27. Kroger provides medical services through The Little Clinic, which has more than 220 locations throughout the states of Arizona, Colorado, Georgia, Indiana, Kansas, Kentucky, Ohio, Tennessee, and Virginia.

28. The website for The Little Clinic states that it "respects the privacy…of all people…."[1]

29. The Little Clinic Bill of Rights and Responsibilities states that patients have the right to "be treated…in a manner that protects privacy and confidentiality of personal information;"[2]

30. The Little Clinic requires that patients provide the following documents: copy of insurance card; proof of ID; and valid form of payment.[3] It also requires that patients provide "accurate and complete information about present complaints, past illnesses, hospitalizations, medications, and other matters related to [their] health;"[4]

31. Kroger also provides prescription drug services through Kroger Pharmacies, of which there are over 2,200 locations nationwide.

32. Kroger requires its customers to provide contact information (such as name, email, and residential address), and financial information (such as Health Services Account or other credit card account information). As part and parcel of providing and/or accepting insurance, customers must also provide their sensitive health information and other personal information (such as dates of birth and Social Security numbers, that Kroger requests).

33. Kroger creates electronic health records of its customers by gathering medical information from them. This information comes from the customers and from other individuals or

[1] https://www.thelittleclinic.com/about-us, last accessed 3/28/2021.
[2] https://www.thelittleclinic.com/topic/patient-bill-of-rights-and-responsibilities, last accessed 3/28/2021.
[3] https://www.thelittleclinic.com/services, last accessed 3/28/2021.
[4] *Id.*

organizations, such as physicians and/or insurance plans.

34. Kroger also provides money services to its customers, such as money orders, check cashing, bill pay, Coinstar, and the ability to send money.[5]

35. Kroger entrusted Accellion, Inc. to hold and possess Kroger's customers' and/or employees' personal data. Accellion is a software company that purports to offer secure file-transfer to its customers. Accellion boasts the security of its "firewall" products that are intended to prevent data breaches: "When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[6]

36. Accellion offers a file-transfer product called "FTA." This self-described "legacy" product is 20 years old[7] and incapable of preventing modern data security threats.

37. Starting April 30, 2021, Accellion will no longer offer its FTA product.[8]

38. For years, Accellion has urged that its customers (such as Kroger) migrate to its newer, more secure product "Kiteworks," which was launched roughly four years ago, yet even though advised to update its security by its own experts Kroger still failed to maintain adequate security.[9]

JURISDICTION & VENUE

39. This Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving more than 100 putative Class Members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

[5] https://www.kroger.com/d/money-services, last accessed 3/28/2021.
[6] https://www.accellion.com/company/
[7] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/
[8] https://www.accellion.com/sites/default/files/resources/fta-eol.pdf
[9] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/; https://www.accellion.com/sites/default/files/resources/fta-eol.pdf

Plaintiff and Kroger are citizens of different states and many members of the putative class are citizens of different states thereby satisfying CAFA's minimal diversity requirement.

40. This Court has general personal jurisdiction over Kroger because Kroger's principal place of business is in Cincinnati, Ohio.

41. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

42. Kroger used Accellion's outdated legacy File Transfer Appliance ("FTA") to transfer the PII (including PHI) of its current and former employees and Health and Money Services customers.

43. Accellion's legacy FTA software relied on CentOS 6 to function.

44. In late 2019, CentOS announced it would no longer support CentOS 6 after November 30, 2020.

45. Upon information and belief, the fact that it was no longer supported by CentOS meant that the FTA software would no longer receive expected vulnerability testing and patching.

46. On December 25, 2020, Accellion suffered a massive data breach which exposed the sensitive PII of millions of individuals—including Kroger's employees and customers.

47. The breach occurred after hackers exploited a vulnerability in Accellion's legacy FTA software through traditional SQL injection methodology.

48. As with all pharmacies and healthcare providers, use of Kroger's health and pharmacy services requires disclosure of PII and PHI to Kroger by all of its health and pharmacy customers.

49. Similarly, as an employer, Kroger required its employees to provide much of the same sensitive PII as its customers.

50. Kroger is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from each Plaintiff or Class Member.

51. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' PII and PHI, Kroger assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII and PHI it collected, stored, and shared with Accellion.

Kroger Knew it Was and Continues to be a Prime Target for Cyberattacks

52. Kroger knew it was an ideal target for hackers and those with nefarious purposes related to consumer, employee, and patient data. They processed and saved multiple types and many levels of PII and PHI.

53. Yet, Kroger did not follow generally accepted industry standards to protect the sensitive PII and PHI entrusted to it.

54. Kroger processed payment information, in addition to all the information about prescription medication, healthcare, and any other information that it might demand as a pharmacy and healthcare provider, such as Social Security number, age, gender, and prior health history. In doing so, Kroger relied upon outdated software from Accellion to transfer such data without adequate security measures.

55. The use of Money Services by Kroger's customers and/or employees similarly required the entrustment of sensitive PII.

56. The seriousness with which Defendant should have taken its data security is shown

by the number of data breaches perpetrated in the healthcare and retail industries in the last few years.

57. Despite knowledge of the prevalence of healthcare and retail data breaches, Defendant failed to prioritize its customers and/or employees' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the millions of sensitive data points of its customers and employees.

58. As a highly successful publicly traded company with a market capitalization of roughly $25 billion, Kroger had the resources to invest in the necessary data security and protection measures, as it was told to do. Yet, it did not—instead, consciously disregarding the known risks and continuing to use Accellion's outdated legacy technology.

59. Defendant failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures presented to Kroger's customers and employees for the first time in late February of 2021, but which occurred in December of 2020.

60. Despite its awareness, Defendant did not take the necessary and required minimal steps to secure Plaintiff's PII and the Class Members' PII and PHI. As a result, hackers breached and stole important PII and PHI from at least hundreds of thousands of Kroger's customers and/or employees.

Kroger Provided Misleading Information to Plaintiff and the Class Members

61. Kroger's letters to Plaintiff and members of the Class were patently deficient because they failed to disclose the full range of information that may have been compromised in the breach, downplayed the risk its customers and employees face as a result of the breach, and

failed to provide customers and employees with important information such as when the breach occurred, how the breach occurred, or the number of individuals affected.

62. For example, the letters received by customers and/or employees state: "We learned that the Accellion incident impacted Kroger's files on January 23, 2021, took immediate action, and we discontinued use of Accellion's services and investigated the scope and impact of the incident." This falsely leads recipients of the letters to believe that the data breach occurred on January 23, 2021. In reality, the breach occurred in December of 2020.

63. The letters also falsely imply that the decision to discontinue Accellion's services was timely and provided a benefit to the customers and employees affected by the breach, when in fact, Kroger had prior knowledge Accellion's services were deficient yet failed to act, and the decision to discontinue Accellion's services had absolutely no impact on the vast amounts of data exposed.

64. The letters downplay the harmful effects to customers and employees of the breach by stating, in the second sentence, that Kroger has "no indication of fraud or misuse of your personal information as a result of this incident." The fact that Kroger itself had not detected fraud or misuse at the time the letter was written is meaningless; customers and employees were (and remain) at imminent risk of identity theft and other fraud—it is common sense that such fraud or misuse was the reason criminals obtained the data in the first place.

65. Furthermore, the fact that Kroger had not detected fraud or misuse does not mean that such incidents had not already occurred—indeed, Kroger's letters encouraged Plaintiff and the Class Members to "[b]e vigilant for the next 12 to 24 months" and told them that if they see suspicious or unusual activity on their accounts, **not to tell Kroger**, but to report it to someone else.

Defendant Owed a Duty to Plaintiff and Class Members to Adequately Safeguard Their PII

66. Defendant is aware of the importance of security in maintaining personal information (particularly medical and financial information), and the value its users place on keeping their PII and PHI secure.

67. Defendant owes a duty to Plaintiff and the Class Members to maintain adequate security and to protect the confidentiality of their personal data.

68. Defendant owes a further duty to its customers and employees to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Sort of PII at Issue Here is Particularly Valuable to Hackers

69. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

70. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

71. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal

> information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[10]

72. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and Class Members stolen in the Kroger security breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Plaintiff's and Class Members' stolen personal data represents essentially one-stop shopping for identity thieves.

73. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[11] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[12]

74. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion

---

[10] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 13, 2020).

[11] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Nov. 13, 2020).

[12] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

detection programs, monitoring data traffic, and having in place a response plan.

75. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

76. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

77. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiff's and Class Members' personal data that was stolen has a high value on both legitimate and black markets.

78. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[14]

79. Individuals rightfully place a high value not only on their PII, but also on the

[13] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited Nov. 13, 2020).
[14] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited Nov. 13, 2020).

privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy – and the amount is considerable.

80. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[15] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

81. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

82. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[16] Former and current Kroger employees and customers whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor

[15] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 14, 2021).
[16] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

their credit and tax filings for an indefinite duration.

83. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Kroger's Post-Breach Activity was Inadequate

84. Personal, health, and financial information can be sold on the black-market almost immediately. As Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's starting to make unauthorized transactions."[17] Thus, the compromised information could be used weeks before the receipt of any letter from Kroger and Kroger's proposed solutions to the potential fraud are, therefore, woefully deficient.

85. Immediate notice of a security breach is essential to protect people such as Plaintiff and the Class Members. Defendant failed to provide such immediate notice, in fact taking roughly two months to disclose to Plaintiff and the Class Members that there had been a breach, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach.

86. Such failure to protect Plaintiff's and the Class Members' PII and PHI, and timely notify of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because many of the data points stolen are persistent—for example, Social Security number, name, address, and medical history—as opposed to transitory—for example, the date of an appointment, criminals who purchase the PII

[17] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last visited Jan. 14, 2021).

and PHI belonging to Plaintiff and the Class Members do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later.

87. A single person's PHI can fetch up to $350 on the dark web. This is due, in part, to the broad scope and comprehensive nature of the data and information, which can be used to steal identities for illegal drug or medical purchases or to defraud insurers. Allowing hackers to steal this type of information is particularly nefarious, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

88. Every year, victims of identity theft lose billions of dollars. And reimbursement is only the beginning, as these victims usually spend hours and hours attempting to repair the impact to their credit, at a minimum.

89. Plaintiff and the Class Members are at constant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the Defendant's actions and the data breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of the breach.

CLASS ACTION ALLEGATIONS

90. Plaintiff brings all claims as Class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the Class defined below.

91. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action

as a national Class action for themselves and all members of the following Class of similarly situated persons:

The Nationwide Class

> All Kroger employees, pharmacy customers, Little Clinic patients, money services customers, and other Kroger customers whose private information was entrusted to Kroger and was compromised in the December 2020 data breach.[18]

92. Excluded from the Class are Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

93. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

94. Certification of Plaintiff's claims for Class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a Class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

95. All members of the proposed Class are readily ascertainable in that Kroger has access to addresses and other contact information for all members of the Class, which can be used to provide notice to Class Members.

96. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes at least hundreds of thousands of individuals whose personal data was entrusted to Kroger and compromised in the Kroger data security breach.

97. ***Commonality***. There are numerous questions of law and fact common to Plaintiff

[18] Plaintiff reserves the right to amend this proposed class definition in the future.

and the Class, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' and/or employees' personal data;
- whether Defendant unreasonably delayed in notifying those affected of the security breach;
- whether Defendant owed a duty to Plaintiff and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the Kroger security breach to Plaintiff and members of the Class;
- whether Defendant breached its duties to protect the personal data of Plaintiff and members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the Kroger security breach to Plaintiff and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant knew or should have known that Accellion's FTA software was vulnerable to attack;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiff and members of the Class that it did not ensure that computers and security practices adequate to reasonably safeguard customers' or employees' financial and personal data were used when handling Plaintiff's and the Class Members' personal data;
- whether Defendant should have notified the public, Plaintiff, and Class Members immediately upon learning of the security breach;
- whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Defendant breached its duties to Plaintiff and the Class as a bailee of PII and/or PHI entrusted to it and for which Defendant owed a duty to safeguard and of safekeeping;
- whether Plaintiff and members of the Class are entitled to recover damages; and
- whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

98. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff,

like all Class Members, had their personal data compromised, breached and stolen in the Kroger security breach. Plaintiff and all Class Members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

99. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

100. ***Predominance***. The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

101. ***Superiority***. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a Class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of Class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a Class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a Class action.

102. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a Class action is superior to other available methods for the fair and

efficient adjudication of this controversy.

103. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action conserves judicial resources and the parties' resources and protects the rights of each Class Member.

COUNT I — NEGLIGENCE

104. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

105. Kroger owed a duty to Plaintiff and Class Members to safeguard their sensitive PII and PHI. As part of this duty, Kroger was required to retain competent third-party data transfer companies to prevent foreseeable harm to Plaintiff and the Class Members, and therefore had a duty to take reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft.

106. In other words, Kroger was required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the personal, health, and financial information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

107. Kroger's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' personal, health, and financial information in its possession was adequately secured and protected.

108. Kroger further owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings

and alerts.

109. There is a very close connection between Kroger's failure to follow reasonable security standards to protect the personal data in its possession and the injury to Plaintiff and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

110. If Kroger had taken reasonable security measures, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Kroger and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect personal data in their possession, they will not take the steps that are necessary to protect against future security breaches.

111. Kroger breached its duties by the conduct alleged in the Complaint by, including without limitation, failing to protect the personal, health, and financial information in its possession; failing to maintain adequate computer systems and data security practices to safeguard the personal, health, and financial information in its possession; failing to utilize adequate, updated, and secure software and related systems to protect the personal, health and financial information in its possession; failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal, health, and financial data from theft; and failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the data breach.

112. As a direct and proximate result of Kroger's failure to exercise reasonable care and

use commercially reasonable security measures, the personal data of Kroger's employees and customers was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

113. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT II — NEGLIGENT ENTRUSTMENT

114. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

115. Kroger owed a duty to Plaintiff and the Class to adequately safeguard the PII and PHI that it required its employees and customers to provide. Part and parcel with this duty was the duty to only entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

116. Kroger breached this duty by entrusting Accellion with the sensitive PII and PHI of its employees' and customers' when, as described throughout the Complaint, it knew or should have known that Accellion and Accellion's legacy FTA software was incompetent at preventing such unauthorized disclosure.

117. As a direct and proximate result of Kroger's failure to exercise reasonable care in whom it entrusted its employees' and customers' sensitive PII and PHI to, the personal data of Kroger's employees and customers was accessed by ill-intentioned criminals who could and will

use the information to commit identity theft or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

118. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT III — BAILMENT

119. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

120. Plaintiff and the Class delivered their personal, health, and financial information to Kroger for the exclusive purpose of obtaining services or employment.

121. The PII and PHI is intangible personal property belonging to Plaintiff and the Class Members.

122. In delivering their personal data to Kroger, Plaintiff and Class Members intended and understood that Kroger would adequately safeguard their personal data, including by exercising reasonable care in whom it provides its employees' and customers' PII and PHI to. For example, The Little Clinic Privacy Policy states that Kroger will "require our business associates to appropriately safeguard…PHI."[19]

123. Kroger understood that it had a duty to account for, return, and/or destroy the PII and PHI entrusted to it upon request. For example, The Little Clinic Privacy Policy states:

[19] https://www.thelittleclinic.com/content/v2/binary/document/tlc/privacy_practices-1609869210750.pdf, last accessed 3/01/2021.

> You have the right to access and copy PHI about you contained in a designated record set for as long as we maintain the PHI. You also have the right to an electronic copy of that information. The designated record set usually will include prescription. [sic] Treatment, and/or billing records. To inspect or copy the designated record set or to receive an electronic copy of PHI about you, you must send a written request.
> …
> You have the right to receive an accounting of the disclosures we have made of PHI about you after April 14, 2003 for most purposes other than treatment, payment, or health care operations.[20]

124. Kroger accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing employment and/or services to Plaintiff and Class Members.

125. A bailment (or deposit) was established for the mutual benefit of the parties.

126. During the bailment (or deposit), Kroger owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal data as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information. Kroger breached this duty when it entrusted its employees' and customers' sensitive PII and PHI to Accellion through the use of Accellion's outdated legacy FTA software, which Kroger knew or should have known was incapable of providing reasonable security to Kroger's data.

127. Kroger breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class Members' personal, health, and financial information.

128. As a proximate result of this conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

[20] *Id.*

COUNT IV — BREACH OF IMPLIED CONTRACT

129. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

130. Plaintiff and the Class delivered their personal, health, and financial information to Kroger as part of the process of obtaining employment or services provided by Kroger.

131. Plaintiff and members of the Class entered into implied contracts with Kroger under which Kroger agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

132. In providing such data, Plaintiff and the other members of the Class entered into an implied contract with Kroger whereby Kroger became obligated to reasonably safeguard Plaintiff's and the other Class Members' sensitive, non-public information.

133. In delivering their personal data to Kroger, Plaintiff and Class Members intended and understood that Kroger would adequately safeguard their personal data.

134. Plaintiff and the Class Members would not have entrusted their private and confidential financial, health, and personal information to Kroger in the absence of such an implied contract.

135. Kroger accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing services or employment to Plaintiff and Class Members.

136. Had Kroger disclosed to Plaintiff and members of the Class that it would entrust such data to incompetent third-party vendors that did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and members of the Class would not have provided their PII and PHI to Kroger.

137. Kroger recognized that its employees' and customers' personal data is highly

sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and members of the Class.

138. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Kroger.

139. Kroger breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their data and instead entrusting such data to Accellion through Accellion's outdated and vulnerable legacy FTA software.

140. As a proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT V — UNJUST ENRICHMENT

141. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

142. Plaintiff and Class Members conferred a monetary benefit on Kroger in the form of monies or fees paid for services from Kroger. Kroger had knowledge of this benefit when it accepted the money from Plaintiff and the Class Members.

143. The monies or fees paid by the Plaintiff and Class Members were supposed to be used by Kroger, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

144. Kroger failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiff and Class Members, instead entrusting such data to Accellion through Accellion's outdated and vulnerable legacy FTA software, and as a result Plaintiff and the Class overpaid Kroger as part of the services they purchased.

145. Kroger failed to disclose to Plaintiff and members of the Class that Accellion's

practices and software and systems (which Kroger chose to utilize) were inadequate to safeguard Plaintiff's and the Class Members PII and PHI against theft.

146. Under principles of equity and good conscience, Kroger should not be permitted to retain the money belonging to Plaintiff and Class Members because Kroger failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' personal, health, and financial information that they paid for but did not receive.

147. Kroger wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

148. Kroger's enrichment at the expense of Plaintiff and Class Members is and was unjust.

149. As a result of Kroger's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Kroger, plus attorneys' fees, costs, and interest thereon.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a Class action on behalf of the Class defined above, appoint Plaintiff as Class representative, and appoint the undersigned counsel as Class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members;

3. Award restitution and damages to Plaintiff and Class Members in an amount to be determined at trial;

4. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Zachary C. Schaengold (0090953)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
zschaengold@msdlegal.com

CHESTNUT CAMBRONNE PA

Bryan L. Bleichner (MN #326689)
100 Washington Ave. So. Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com

Counsel for Plaintiff and the Class